SPYWOLF

Security Audit Report

Completed on
April 16, 2023

OVERVIEW

This audit has been prepared for **ShibAnon** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

"

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

– SPYWOLF Team –

TABLE OF CONTENTS

ShibAnon

PROJECT DESCRIPTION

According to their litepaper:

Shibanon was created to become the first mixer on the Shibarium chain. Staying true to the core essence of decentralization, Shibanon will provide ultimate privacy to your transactions while utilizing their platform. The purpose of this unique mixer dApp executing this function, is to ensure investors on the Shibarium chain maintain their privacy with every transaction.

Release Date: Presale starts in April, 2023
Category: Crypto mixer

01

CONTRACT INFO

Token Name
ShibAnon

Symbol
$Shibanon

Contract Address
0x57852e8e787ff5af7c0E1d0b156ec491eC78Ec92

Network
Ethereum

Language
Solidity

Deployment Date
Nov 10, 2022

Verified?
Yes

Total Supply
1,000,000,000

Status
Not launched

TAXES

Buy Tax
5%

Sell Tax
5%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	1000000000 $Shibanon
Median Transfer Amount	1000000000 $Shibanon
Average Transfer Amount	1000000000 $Shibanon
First transfer date	2023-04-10
Last transfer date	2023-04-10
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-04-10 22:26:11 UTC
Created	2023-04-10 22:26:11 UTC
Create TX	0x430569c4eabc1e2897d976b246e7f30120ba154bfc0247cb36f1ddb6158829ff
Creator	0xcb8436363d1d351a8a18b4435782cd60497f1aa8

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

04

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.
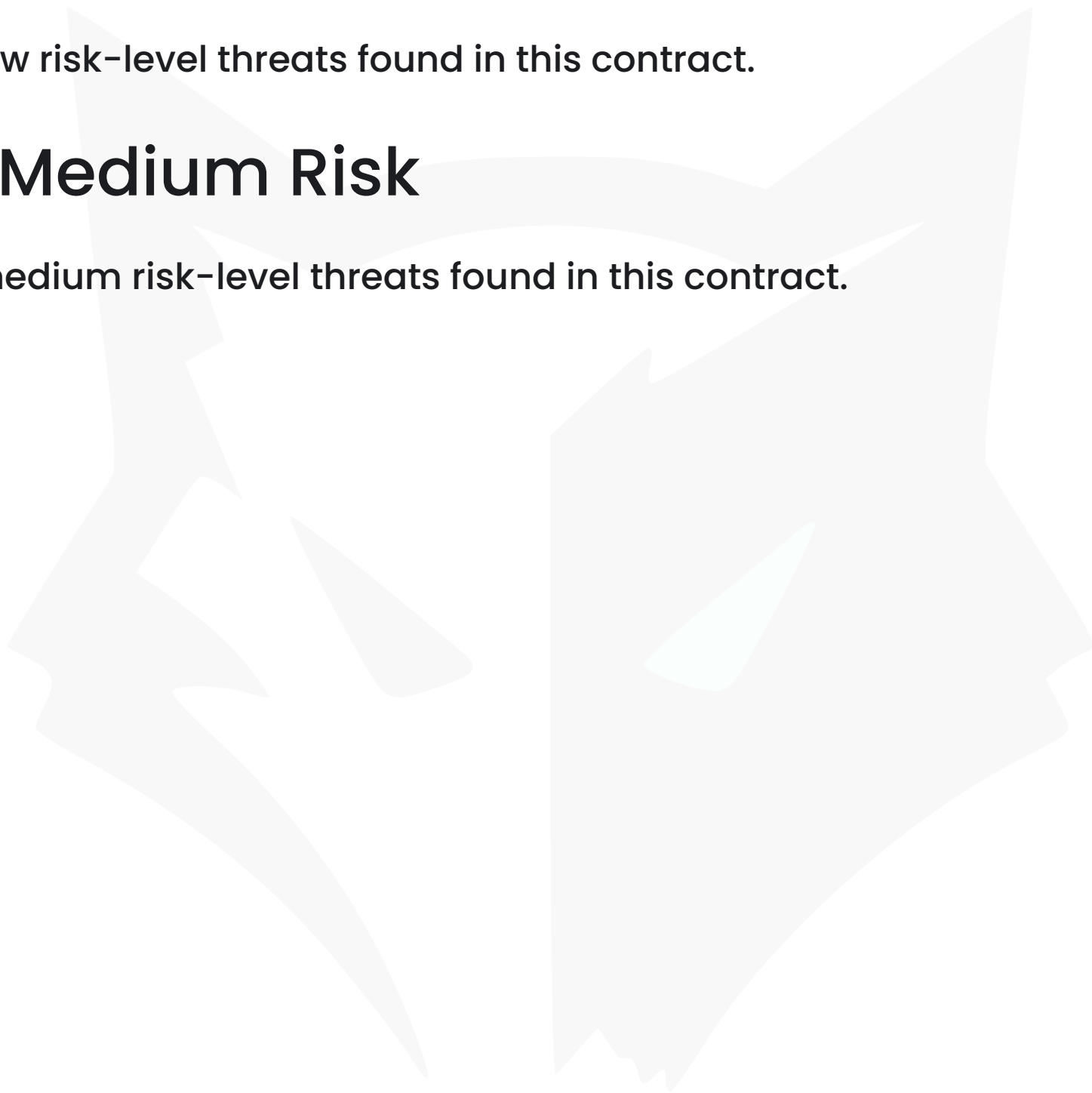
FOUND THREATS

⚠️ Low Risk

No low risk-level threats found in this contract.

⚠️ Medium Risk

No medium risk-level threats found in this contract.

06-A

FOUND THREATS

⚠️ High Risk

Owner can set contract's autoswap threshold.
If minimumTokensBeforeSwap state variable is set to 0 or very low number and swapAndLiquifyByLimitOnly variable is set to true, selling will fail for all users.

```solidity
function setNumTokensBeforeSwap(uint256 newLimit) external onlyOwner() {
    minimumTokensBeforeSwap = newLimit;
}

function _transfer(address sender, address recipient, uint256 amount) private returns (bool) {
......................
if (overMinimumTokenBalance && !inSwapAndLiquify && !isMarketPair[sender] && swapAndLiquifyEnabled)
{
    if(swapAndLiquifyByLimitOnly)
        contractTokenBalance = minimumTokensBeforeSwap;
    swapAndLiquify(contractTokenBalance);
}
...................
}
```

- Recommendation:
  - Ensure that 'minimumTokensBeforeSwap' state variable is always above 1 token (consider token decimals).

06-B

FOUND THREATS

⚠️ High Risk

Owner can turn on/off max wallet limit check.
If wallet limit check is on, max wallet limit is below liquidity pair's balances and the liquidity paid address is not excluded from max wallet, trading will fail.

```solidity
function enableDisableWalletLimit(bool newValue) external onlyOwner {
    checkWalletLimit = newValue;
}

function setWalletLimit(uint256 newLimit) external onlyOwner {
    _walletMax  = newLimit;
}

function _transfer(address sender, address recipient, uint256 amount) private returns (bool) {
.....................
if(checkWalletLimit && !isWalletLimitExempt[recipient]) {
    require(balanceOf(recipient).add(finalAmount) <= _walletMax,"Amount Exceed From Max Wallet Limit!!");
}
.....................
}
```

- Recommendation:
    - Ensure that liquidity pair address is always excluded from max wallet restrictions and/or transfers to liquidity pair are out of check's scope.

06-C

SPYWOLF.CO

⚠️ High Risk

Owner can set max transaction limit without limitations. If max transaction limit is set to 0, trading will fail to users not excluded from such limits .

```
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner() {
    _maxTxAmount = maxTxAmount;
}

function _transfer(address sender, address recipient, uint256 amount) private returns (bool) {
.....................
if(!isTxLimitExempt[sender] && !isTxLimitExempt[recipient] && EnableTransactionLimit) {
    require(amount <= _maxTxAmount, "Transfer amount exceeds the maxTxAmount.");
}
.....................
}
```

- Recommendation:
  - Considered as good tax limit practice is max transaction limit to be not lower than 0.1% of total supply.

06-D

ℹ️ Informational

Owner can withdraw any tokens from the contract.
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.
Owner can withdraw BNB from the contract.

```solidity
function rescueStuckedToken(address _token, uint _amount) external onlyOwner {
    IERC20(_token).transfer(msg.sender,_amount);
}

function rescueFunds() external onlyOwner {
    (bool os,) = payable(msg.sender).call{value: address(this).balance}("");
    require(os);
}
```

Owner can exclude address from fees, transaction limit and max wallet limit. When address is excluded from such restrictions, the user can transfer and receive the whole amount of the bought, sold and/or transferred tokens.

```solidity
function setIsTxLimitExempt(address holder, bool exempt) external onlyOwner {
    isTxLimitExempt[holder] = exempt;
}

function setIsExcludedFromFee(address account, bool newValue) public onlyOwner {
    isExcludedFromFee[account] = newValue;
}

function setIsWalletLimitExempt(address holder, bool exempt) external onlyOwner {
    isWalletLimitExempt[holder] = exempt;
}
```

06-E

ℹ️ Informational

*Owner can set buy/sell taxes up to 4%.
Combined buy+sell = 8%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make. Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```solidity
uint256 public feeUnits = 100;

function setBuyTaxes(uint _Liquidity, uint _Marketing , uint _Developer) public onlyOwner {
    _buyLiquidityFee = _Liquidity;
    _buyMarketingFee = _Marketing;
    _buyDeveloperFee = _Developer;
    _totalTaxIfBuying = _buyLiquidityFee.add(_buyMarketingFee).add(_buyDeveloperFee);
    require(_totalTaxIfBuying <= (feeUnits/25), "Buy fees must be 25% or less");
}

function setSellTaxes(uint _Liquidity, uint _Marketing , uint _Developer) public onlyOwner {
    _sellLiquidityFee = _Liquidity;
    _sellMarketingFee = _Marketing;
    _sellDeveloperFee = _Developer;
    _totalTaxIfSelling = _sellLiquidityFee.add(_sellMarketingFee).add(_sellDeveloperFee);
    require(_totalTaxIfSelling <= (feeUnits/25), "Sell fees must be 25% or less");
}
```

*Note:
Revert comment states 25%, if 25% is intended feeUnits should be divided by 4.

Considered as good tax fee deduction practice is buy and sell fees **combined** not to exceed 25%.

06-F

RECOMMENDATIONS FOR
GOOD
PRACTICES

ShibAnon
GOOD PRACTICES FOUND

1 Consider fundamental tradeoffs

2 Be attentive to blockchain properties

3 Ensure careful rollouts

4 Keep contracts simple

5 Stay up to date and track development

✔ The owner cannot mint new tokens after deployment

✔ The smart contract utilizes "SafeMath" to prevent overflows

There is no information about initial tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS

WEBSITE

Website URL
https://www.shibanon.com/

Domain Registry
https://www.godaddy.com

Domain Expiration
Expires on 2024-03-22

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.
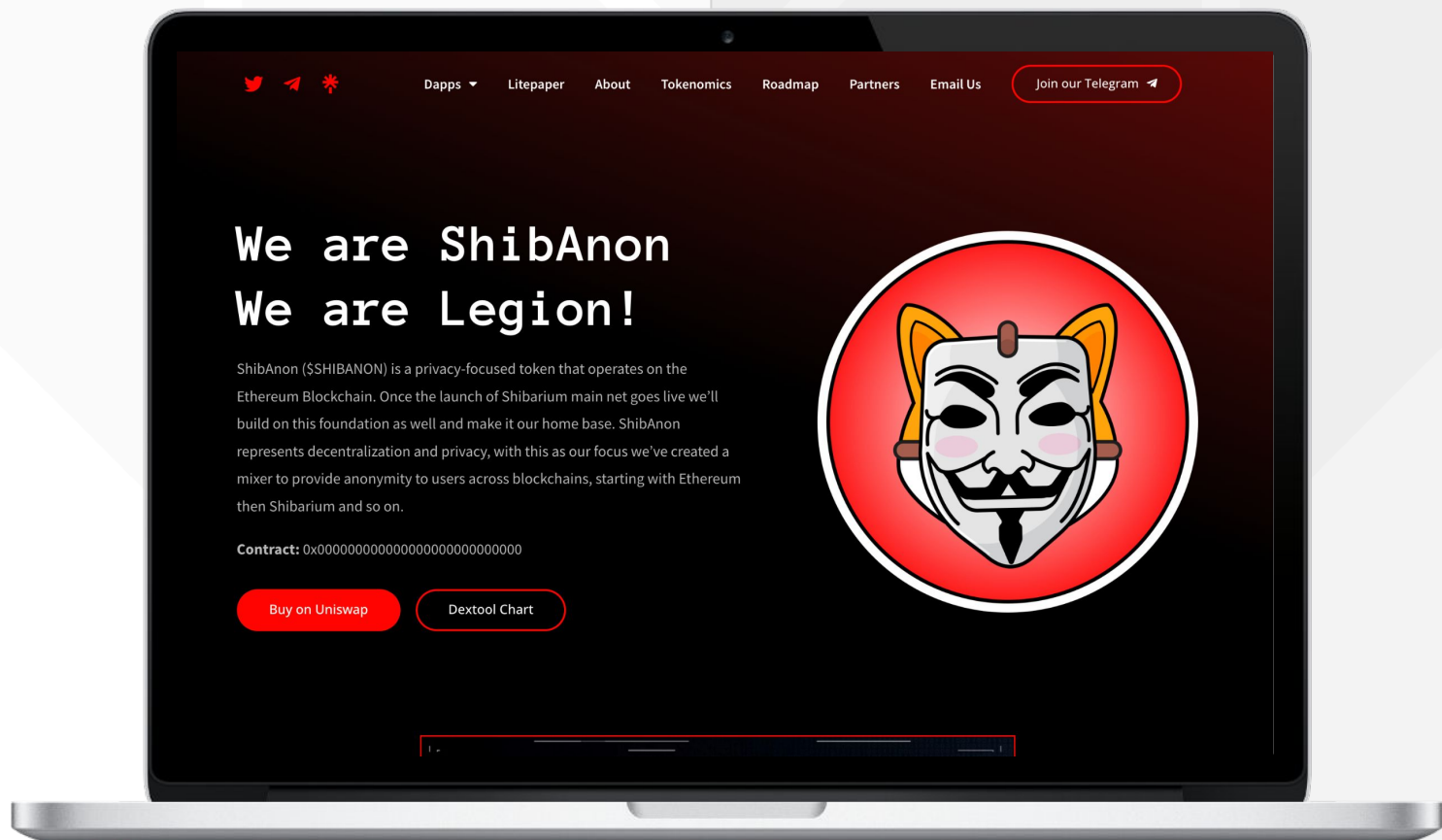
Whitepaper
Well written, explanatory.

Roadmap
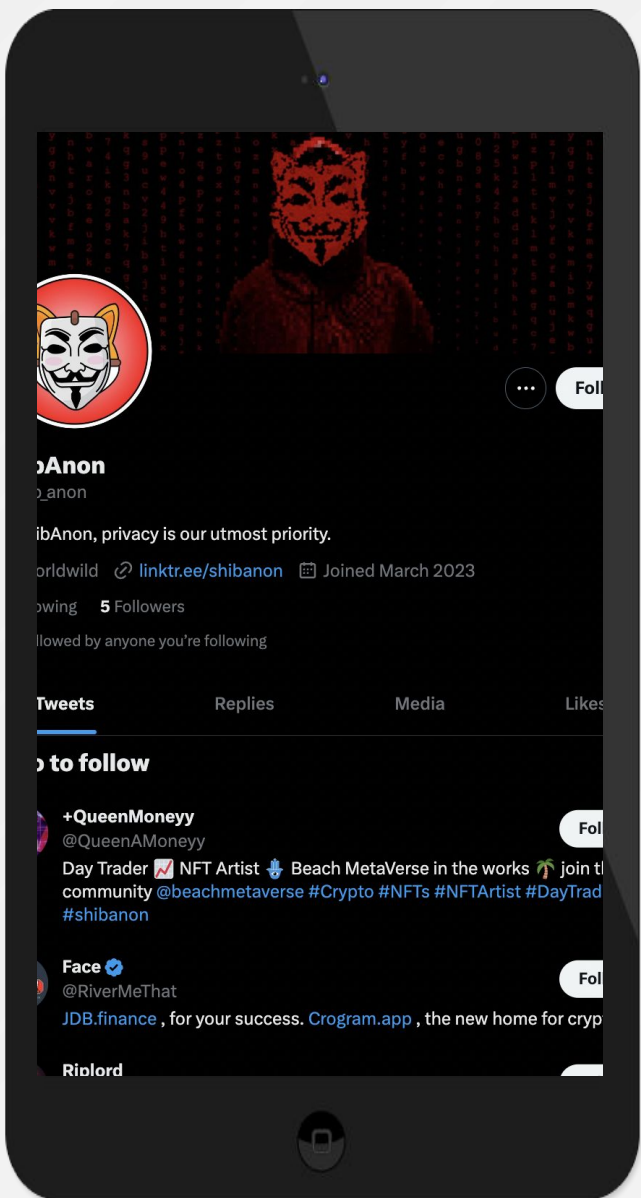Yes, goals set without time frames.

Mobile-friendly?
Yes

Twitter | Telegram | Dapps ▾ | Litepaper | About | Tokenomics | Roadmap | Partners | Email Us | Join our Telegram

We are ShibAnon
We are Legion!

ShibAnon ($SHIBANON) is a privacy-focused token that operates on the Ethereum Blockchain. Once the launch of Shibarium main net goes live we'll build on this foundation as well and make it our home base. ShibAnon represents decentralization and privacy, with this as our focus we've created a mixer to provide anonymity to users across blockchains, starting with Ethereum then Shibarium and so on.

Contract: 0x0000000000000000000000000000000000

Buy on Uniswap | Dextool Chart

shibanon.com

09

SOCIAL MEDIA

& ONLINE PRESENCE

Twitter

- Not available

Discord

- Not available

Telegram

- Not available

Medium

- Not available

10

SPYWOLF
CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✔ **OVER 400 SUCCESSFUL CLIENTS**

- ✔ **MORE THAN 500 SCAMS EXPOSED**

- ✔ **MILLIONS SAVED IN POTENTIAL FRAUD**

- ✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**

- ✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 **SPYWOLF.CO**

✈ **@SPYWOLFNETWORK**

🐦 **@SPYWOLFNETWORK**

11

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.